УДК 343.1:65.012.8+004
КАЛАНЧА Андрій Андрійович,
курсант 1 курсу факультету № 4
Харківського національного університету внутрішніх справ;
КЛІМУШИН Петро Сергійович,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій і кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-1020-9399

АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ ЯК СПОСІБ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

На сьогодні спостерігається стрімкий зріст об'єму мережевого трафіку, що провокує ускладнення його структури. Аналіз мережевого трафіку набуває все більшу актуальність у зв'язку з розвитком мережевих технологій, впровадженням великої кількості нових мережевих протоколів, збільшенням обсягу мережевих даних. Практичне застосування моніторингу мережі забезпечує: виявлення проблем в роботі мережі; запобігання мережевих атак; визначення класифікації трафіку. Моніторинг трафіку також необхідний, щоб більш ефективно діагностувати, оптимізувати пропускну здатність каналів передачі даних, контролювати якість зв'язку та вирішувати проблеми в сфері протидії кіберзлочинності.

Метою роботи є визначення інструментів аналізу мережевого трафіку та порівняльна оцінка їх можливостей в протидії кіберзлочинності.

У кіберполіції для розслідування злочинів необхідні знання з форензики (комп'ютерна криміналістика, розслідування кіберзлочинів), аналізаторів мережевого траіфіку (сніферів), методів атак та криптографії. Моніторинг мережі складне завдання, що вимагає великих сил та витрат, яке є невід'ємною складовою повсякденного життя мережевих адміністраторів-провайдерів мережі. Проте левову частку від успішності цих розслідувань грає саме провайдер, оскільки у нього міститься вся інформація про дії злочинця у мережі. Провайдери мають доступ до такої інформації: усі відвідані сайти з протоколом http/https; завантажені дані; трафік і дані з месенджерів. Ключовим моментом є, на теперішній час, відсутність безпосередньої комунікації між провайдерами та кіберполіцією. Тож досить часто доводиться власноруч перехоплювати трафік та слідкувати за мережевою активністю підозрюваного.

Сьогодні на ринку є інструменти моніторингу як платні так і безкоштовні. І хоча кожен інструмент побудований на основних принципах збору мережевого трафіку, вони значно відрізняються за своєю шириною та глибиною.

TCPDump це інструмент дослідження пакетів з відкритим кодом, сумісний на платформах Unix та Linux, більш легкий і портативний інструмент для сніфу пакетів і тому мережеві адміністратори використовують його для доступу до мережевих пристроїв з віддаленого місця. Обмеженнями TCPDump є: відсутність візуального захоплення даних; застосовування для аналізу протоколів лише на основі TCP; пакети, заблоковані брандмауером, не відображаються.

Colasoft це інструмент аналізатора протоколів із закритим кодом, що використовується для усунення несправностей, порушень та моніторингу трафіку в мережі. Він забезпечує: простоту використання; глибокий аналіз пакетів у режимі реального часу та надійний поглиблений, криміналістичний аналіз протоколів; має особливість відкриття декількох графічних інтерфейсів та можливість генерування різноманітних звітів. Є деякі обмеження Colasoft: це дорогий додаток, що працює лише на платформі операційної системи Microsoft Windows [1].

Wireshark є проектом програмного забезпечення з відкритим вихідним кодом і випущено під загальною суспільною ліцензією GNU (GPL), доступній для UNIX і Windows і надає наступні функції: знімає пакетні дані в реальному часі з мережевого інтерфейсу; відкриває файли, що містять пакетні дані; імпортує пакети з текстових файлів; відображає пакети з дуже детальною інформацією про протокол; зберігає зібрані пакетні дані; експортує пакети; фільтрує пакети та виконує пошук пакетів за багатьма критеріями; створює різноманітні ста-

тистичні дані. Обмеження Wireshark: потребує найкращого розуміння форматів протоколів; знання мови у форматі байтів; не є автоматизованим інструментом та не підтримує моніторинг в тривалому часі [2].

Для порівняння наданих інструментів мережевого аналізу слідує використовувати таки параметри, як тип вихідного коду, кількість підтримуваних протоколів, підтримувана операційна система, вартість, форми декодування тощо.

Colasoft має функції аналізу більш візуального пояснення зі статистикою захоплених пакетів, відображенням більшої кількості інформації про протоколи та користувацькі програми з графіками та матричним поданням для всіх підключених кінцевих точок. Colasoft, у порівнянні з Wireshark, забезпечує більшу мережеву безпеку. Проте, він охоплює лише 300 протоколів, що дуже менше порівняно з Wireshark, який підтримує 1100 протоколів. TCPDump - це дуже портативний і економічний пакет.

Таким чином, аналіз інструментів моніторингу мережевого трафіку показав, що Wireshark, Colasoft є досить ефективними інструментами в протидії кіберзлочинності, а завдяки своїй доступності Wireshark надає для кіберполіції широкі можливості аналізу множини протоколів, що прискорить розслідування протиправних діянь в кіберпросторі.

Список використаних джерел

1. Горбовський А. І., Войтович О. П. Дослідження безпеки у інтернеті речей // Матеріали XLVI науково-технічної конференції підрозділів ВНТУ, Вінниця, 22-24 березня 2017 р. URL: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/17277/2805.pdf?sequence=3 (дата звернення: 23.04.2021).

2. Smarter Security For Your Everything, Atmel Has You Covered // Microchip : вебсайт. 2019. URL: https://www.microchip.com/design-centers/security-ics (дата звернення: 23.04.2021).

3. Асангханва Ю., Ий Р., Сыров А. Повышение уровня безопасности граничных узлов интернета вещей с помощью микросхем ATECC608A компании microchip. *Электроника НТБ*. 2019. № 7 (00188). С. 60-64.

Одержано 18.04.2022

УДК 343.1:65.012.8+004

КАЛАНЧА Андрій Андрійович,
курсант 1 курсу факультету № 4
Харківського національного університету внутрішніх справ;
СВІТЛИЧНИЙ Віталій Анатолійович,
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-3381-3350

АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ ЯК СПОСІБ ПРОТИДІЇ ЗЛОЧИННОСТІ

Дедалі більше люди використовують Інтернет та техніку в повсякденному житті: розумні холодильники аналізують термін придатності продуктів, нагадують, що потрібно придбати в магазині; розумні чайники самі вмикаються за вашої присутності поряд, а жалюзі зачиняються в темну пору доби. У кожного «розумного» пристрою є доступ до Всесвітньої мережі, а кожен такий девайс має власну IP-/MAC-адресу, що дозволяє власнику керувати ними дистанційно. Проте постає запитання, чи залишається ця інформація лише на цьому пристрої, та чи не протікає вона у чиїсь злі руки?

Великі корпорації типу Google чи Amazon вже вирішили за Вас, що б Ви хотіли придбати, яке місце Ви б хотіли відвідати для прогулянки чи затишної вечері зі своєю другою половинкою [1].